

REMARKS

Claims 1 through 8, and 15 through 39 have been examined and stand rejected. Claims 1, 2, 6, 7, 15-18, 21-29, and 31-39 were rejected under 35 U.S.C. § 102(e) as allegedly being anticipated by U.S. Patent 5,915,023 (“Bernstein”). Claims 3, 4, and 19 were rejected under 35 U.S.C. § 103(a) as allegedly being obvious over Bernstein in view of U.S. Patent 5,915,023 (“McKinsey”). Claims 5, 8, 20 and 30 were rejected under 35 U.S.C. § 103(a) as allegedly being unpatentable over Bernstein in view of what the Examiner asserts would have been obvious to one of ordinary skill in the art.

By this amendment, Applicant cancels claims 32, 33 and 36. The remaining pending claims are 1 through 8, 15 through 31, 34, 35, and 37 through 39.

Applicant has amended claims 1, 6, 21, 24 and 34. In view of the Applicant’s amendments and the remarks that follow, Applicant respectfully requests reconsideration of the rejection and allowance of the now pending claims.

I. Rejections Under Section 102(e) of Pending Claims 1, 2, 6, 7, 15-18, 21-29, 31, 34, 35, and 37-39

The Examiner has rejected claims 1, 2, 6, 7, 15-18, 21-29, 31, 34, 35, and 37-39, asserting that these claims are anticipated by Bernstein. Applicant respectfully disagrees. Bernstein fails to disclose at least one limitation of each of these claims and, consequently, the Examiner’s rejection of them should be withdrawn.

A. Overview of Bernstein

Bernstein is generally directed to an apparatus and method for securely transferring “value” (*e.g.*, payment) from a transferor (*e.g.*, a purchaser of goods) to a transferee (*e.g.*, a vendor of goods) over the public service telephone network (“PSTN”). *See* Col. 2, ll. 33-35; and

Col. 3, ll. 27-30. In the embodiments described by Bernstein, this value may be transferred via two modes of payment: a direct value transfer, which is similar to the transfer of electronic cash but without the assistance of a financial institution (*see* Col. 3, ll. 31-37); or by credit or transferring cash from a financial institution account of the authorized user to a financial institution account of the vendor (*see* Col. 3, ll. 64-67).

According to Bernstein, whatever the mode of payment used, the transferor must first uniquely identify itself to the financial institution that will be transferring value from the transferor's account to that of the transferee. (*See* Col. 4, ll. 20-24). To ensure security, Bernstein discloses, in one embodiment, the following steps.

First, the transferor transmits an identifier (*e.g.*, an account number) that uniquely identifies the transferor to the transferor's financial institution. (*See* Col. 4, ll. 27-29). Next, once the transferor has been identified, the financial institution uses such identification to access a file of the authorized user for a set of encryption keys to decode subsequent transmissions from the transferor. *Id.*, at ll. 29-34. Then, the transferor, using an identical set of encryption keys, encodes further indicia of identity, such as, for example, a PIN number, for transmission to the financial institution, and which may only be decoded by the financial institution. (*Id.*, at ll. 34-37). The transferor may also encode and transmit to the financial institution other information, such as mode of payment and payment amount. (*Id.*, at ll. 37-40). Finally, the financial institution, on decoding the transmission, responds in the clear (*i.e.*, no encryption) with an acceptance or rejection message, or with a request for re-transmission if an error occurred. (*Id.*, at ll. 40-43).

Notably, in Bernstein the transferor's financial institution is responsible for, and capable of, decrypting both PIN and non-PIN encrypted information sent to it by the transferor.

B. Claims 1 and 2

Among its limitations, independent claim 1, as amended, requires the step of “transmitting the cryptographically isolated PIN data and non-PIN data over the network to a remote location *having only the capability to decode the second encryption operation.*” (Emphasis supplied). Nowhere in Bernstein is such a limitation disclosed or suggested. Rather, in Bernstein both the encrypted PIN and encrypted non-PIN data are transmitted to a single remote location that decodes both the PIN and non-PIN data, such as, for example, the transferor’s financial institution (*see* Col. 8, ln. 39 – Col. 9, ln. 22) or third party agent (*see* Col. 12, ll. 34-44).

Thus, it is respectfully submitted that Bernstein does not anticipate independent claim 1. Moreover, it is respectfully submitted that since claim 2 depends from, and includes all of the limitations of, claim 1, Bernstein does not anticipate claim 2 either.

C. Claims 6 and 7

Among its limitations, independent claim 6, as amended, requires the steps of:

- receiving the encrypted transaction data from a first remote location over a network having at least a public component;
- performing at the first remote location, a first decryption operation to decode only the encrypted non-PIN data; ~~and~~
- transmitting at least the encrypted account PIN data to a second remote location; and
- performing at the second remote location a second decryption operation to decode the encrypted account PIN data, wherein said second decryption operation is different from the first decryption operation.

Thus, independent claim 6 requires that at a first network location a first decryption operation be performed to decrypt only the non-PIN data, and that at a second network location, a second, different, decryption operation be performed to decode the PIN data. Nowhere in

Bernstein are these limitations disclosed or suggested. Rather, in Bernstein both the encrypted PIN and encrypted non-PIN data are transmitted to a single remote location that decodes both the PIN and non-PIN data, such as, for example, the transferor's financial institution (*see* Col. 8, ln. 39 – Col. 9, ln. 22) or third party agent (*see* Col. 12, ll. 34-44).

Thus, it is respectfully submitted that Bernstein does not anticipate independent claim 6. Moreover, it is respectfully submitted that since claim 7 depends from, and includes all of the limitations of, claim 6, Bernstein does not anticipate claim 7 either.

D. Claims 15 through 18

Among its limitations, independent claim 15 requires the steps of:

transmitting the encrypted PIN and non-PIN data over a data network to an authentication requestor at a remote location, said authentication requestor having means to decrypt only the non-PIN data;

transmitting the encrypted PIN data over a data network to an authorizing agent for verification; [and]

decrypting and verifying the PIN data by the authorizing agent . . .

Nowhere in Bernstein is it either disclosed or suggested that the encrypted PIN and non-PIN data are transmitted to an authentication requestor having means to decrypt only the non-PIN data, as is required by independent claim 15. Bernstein further fails to disclose or suggest that the encrypted PIN data is transmitted to a separate authorizing agent for verification.

Rather, in Bernstein both the encrypted PIN and encrypted non-PIN data are transmitted to a single remote location that decodes both the PIN and non-PIN data, such as, for example, the transferor's financial institution (*see* Col. 8, ln. 39 – Col. 9, ln. 22) or third party agent (*see* Col. 12, ll. 34-44).

Thus, it is respectfully submitted that Bernstein does not anticipate independent claim 15. Moreover, it is respectfully submitted that since claims 16 through 18 depend from, and include all of the limitations of, claim 15, Bernstein fails to anticipate those claims as well.

E. Claims 21 through 23

Among its limitations, independent claim 21 requires:

means for performing a second encryption operation on at least the non-PIN data, such that the PIN data is cryptographically isolated from the non-PIN data;

means for transmitting the cryptographically isolated PIN data and non-PIN data over a data network to a remote location; and

transmitting the cryptographically isolated PIN data and non-PIN data over the network to a remote location having only the capability to decode the second encryption operation.

Nowhere in Bernstein is it either disclosed or suggested that the cryptographically isolated PIN data and non-PIN data be both transmitted to a remote location having the capability to decode only the second encryption operation, as is required by independent claim 21. Rather, in Bernstein both the encrypted PIN and encrypted non-PIN data are transmitted to a single remote location that decodes both the PIN and non-PIN data, such as, for example, the transferor's financial institution (*see* Col. 8, ln. 39 – Col. 9, ln. 22) or third party agent (*see* Col. 12, ll. 34-44).

Thus, it is respectfully submitted that Bernstein does not anticipate independent claim 21. Moreover, it is respectfully submitted that since claims 22 and 23 depend from, and include all of the limitations of, claim 21, Bernstein fails to anticipate claims 22 and 23 as well.

F. Claims 24, 25 and 31

Among its limitations, independent claim 24, as amended, requires:

means for transmitting at least the encrypted account PIN data to a second remote location; and

means for performing at the second remote location a second decryption operation to decode the encrypted account PIN data, wherein said second decryption operation is different from the first decryption operation.

Nowhere in Bernstein are these limitations disclosed or suggested. Rather, in Bernstein both the encrypted PIN and encrypted non-PIN data are transmitted to a single remote location that decodes both the PIN and non-PIN data, such as, for example, the transferor's financial institution (*see* Col. 8, ln. 39 – Col. 9, ln. 22) or third party agent (*see* Col. 12, ll. 34-44).

Thus, it is respectfully submitted that Bernstein does not anticipate independent claim 24. Moreover, it is respectfully submitted that since claims 25 and 31 depend from, and include all of the limitations of, claim 24, Bernstein does not anticipate claims 25 and 31 either.

G. Claims 26 through 29

Among its limitations, independent claim 26 requires:

means for transmitting the encrypted PIN and non-PIN data over a data network to an authentication requestor, said authentication requestor having means to decrypt only the non-PIN data;

means for transmitting the encrypted PIN data over a data network to an authorizing agent for verification;

means for decrypting and verifying the PIN data by the authorizing agent . . .

Nowhere in Bernstein is it either disclosed or suggested that the encrypted PIN and non-PIN data are transmitted to an authentication requestor having means to decrypt only the non-PIN data, as is required by independent claim 26. Bernstein further fails to disclose or suggest that the encrypted PIN data is transmitted to a separate authorizing agent for verification.

Rather, in Bernstein both the encrypted PIN and encrypted non-PIN data are transmitted to a single remote location that decodes both the PIN and non-PIN data, such as, for example, the

transferor's financial institution (*see* Col. 8, ln. 39 – Col. 9, ln. 22) or third party agent (*see* Col. 12, ll. 34-44).

Thus, it is respectfully submitted that Bernstein does not anticipate independent claim 26. Moreover, it is respectfully submitted that since claims 27 through 29 depend from, and include all of the limitations of, claim 26, Bernstein fails to anticipate those claims as well.

H. Claims 34, 35 and 37

Among its limitations, independent claim 34 requires:

receiving the transaction data from a remote location over a network having at least a public component, wherein said remote location does not have the capability to decode the encrypted PIN data;

performing a first decryption operation to decode the encrypted non-PIN data; and

transmitting at least said encrypted PIN data to another remote location.

Bernstein neither discloses nor suggests a remote location that receives transaction data and that does not have the capability of decoding encrypted PIN data. Nor does Bernstein disclose or suggest transmitting at least the encrypted PIN data to another remote location. Rather, in Bernstein both the encrypted PIN and encrypted non-PIN data are transmitted to a single remote location that decodes both the PIN and non-PIN data, such as, for example, the transferor's financial institution (*see* Col. 8, ln. 39 – Col. 9, ln. 22) or third party agent (*see* Col. 12, ll. 34-44).

Thus, it is respectfully submitted that Bernstein does not anticipate independent claim 34. Moreover, it is respectfully submitted that since claims 35 and 37 depend from, and include all of the limitations of, claim 34, Bernstein fails to anticipate those claims as well.

I. Claim 38

Among its limitations, claim 35 requires:

performing a decryption operation on at least a portion of the encrypted non-PIN data resulting in at least some unencrypted non-PIN data;

transmitting the encrypted PIN data and at least the unencrypted non-PIN data over the data network to an authorizing agent having means to decrypt the encrypted PIN data . . .

Bernstein neither suggests nor discloses these limitations. Rather, in Bernstein both the encrypted PIN and encrypted non-PIN data are transmitted to a single remote location that decodes both the PIN and non-PIN data, such as, for example, the transferor's financial institution (*see* Col. 8, ln. 39 – Col. 9, ln. 22) or third party agent (*see* Col. 12, ll. 34-44).

Thus, it is respectfully submitted that Bernstein does not anticipate claim 38.

H. Claim 39

Among its limitations, claim 39 requires “an authorization requestor, and an authorizing agent, wherein the user has the capability of encrypting PIN data and non-PIN data using different encryption operations, the authorization requestor has the capability of decoding only the non-PIN data, and the authorizing agent has the capability of decoding the PIN data . . .”

Bernstein neither discloses nor suggests these limitations. Rather, in Bernstein both the encrypted PIN and encrypted non-PIN data are transmitted to a single remote location that decodes both the PIN and non-PIN data, such as, for example, the transferor's financial institution (*see* Col. 8, ln. 39 – Col. 9, ln. 22) or third party agent (*see* Col. 12, ll. 34-44).

Thus, it is respectfully submitted that Bernstein does not anticipate claim 39.

II. Rejections Under Section 103(a) of Claims 3, 4 and 19

Claims 3, 4 and 19 were rejected under Section 103(a) as being obvious over Bernstein in view of McKinsey.

Claims 3 and 4 depend from, and include all of the limitations of, claim 1. As previously explained, Bernstein is deficient as a reference with respect to claim 1. Consequently, Bernstein

is deficient with respect to claims 3 and 4 as well. Furthermore, claim 19 ultimately depends from, and includes all of the limitations of, claim 15, and, as was previously explained, Bernstein is deficient as a reference with respect to claim 15. Consequently, Bernstein is also deficient with respect to claim 15.

McKinsey does not cure the deficiencies of Bernstein with respect to claims 3, 4 and 19, nor was McKinsey cited by the Examiner for that purpose. Rather, McKinsey was cited as allegedly disclosing other additional limitations in these claims. Thus, even if McKinsey does disclose those additional limitations – and Applicant does not concede that it does – the combination of McKinsey and Bernstein remains deficient with respect to claims 3, 4, and 19. It is respectfully submitted that the rejection of claims 3, 4 and 19 under Section 103(a) should be withdrawn.

III. Rejections Under Section 103(a) of Claims 5, 8, 20 and 30

Claims 5, 8, 20 and 30 were rejected under Section 103(a) as being obvious over Bernstein in view of the Examiner's "official notice" that one-way hash functions are well-known to those of ordinary skill in the art.

Claim 5 depends from, and includes all of the limitations of, claim 1. As previously explained, Bernstein is deficient as a reference with respect to claim 1. Consequently, Bernstein is also deficient with respect to claim 5. Furthermore, claim 8 depends from claim 6, claim 20 ultimately depends from claim 15, and claim 30 depends from claim 26. As previously explained, Bernstein is deficient as a reference with respect to base claims 6, 15, and 26. Thus, Bernstein is also deficient with respect to dependent claims 8, 20 and 30.

The Examiner has taken "official notice" that one-way hash functions are well-known to one of ordinary skill in the art, and asserts that one-way hash functions are all that is additionally

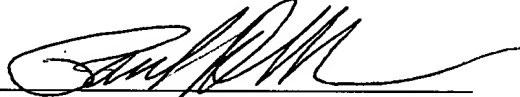
claimed by claims 5, 8, 20 and 30. Assuming, for the sake of argument, that the Examiner is correct, common knowledge of one-way hash functions by those of ordinary skill in the art fails to cure the deficiencies of Bernstein with respect to claims 5, 8, 20 and 30. It is therefore respectfully submitted that the Examiner's rejection of claims 5, 8, 20 and 30 under Section 103(a) should be withdrawn.

IV. Conclusion

For the reasons set forth above, applicant respectfully submits that this application is now in condition for allowance. Reconsideration and prompt allowance of all presently pending claims are respectfully requested.

Respectfully submitted,

BAKER BOTTS L.L.P.



Paul D. Ackerman

Patent Office Reg. No. 39,891

Dated: March 29, 2005

BAKER BOTTS L.L.P.

30 Rockefeller Plaza

New York, NY 10112-4498

Attorney for Applicants

212-408-2512